Configuration Guide | PUBLIC

2024-02-13

Quick Configuration Guide for the ILM Store

Version for Microsoft Azure

THE BEST RUN

Content

1 Introduction

The SAP Information Lifecycle Management (ILM) Store enables you to run the entire data retention process from data archiving and storing to their destruction, thus enabling data management through its lifecycle. This process takes into consideration SAP ILM Retention Management (RM) specifications.

You can use the WebDAV interface standard to store archive files in a Microsoft Azure storage account using Blob storage. This guide explains how to configure the ILM Store with a Microsoft Azure Blob storage account.

> ⓘ Note
>
> This is a quick setup guide. For extensive documentation, refer to the Installation and Configuration Guide fot the ILM Store.

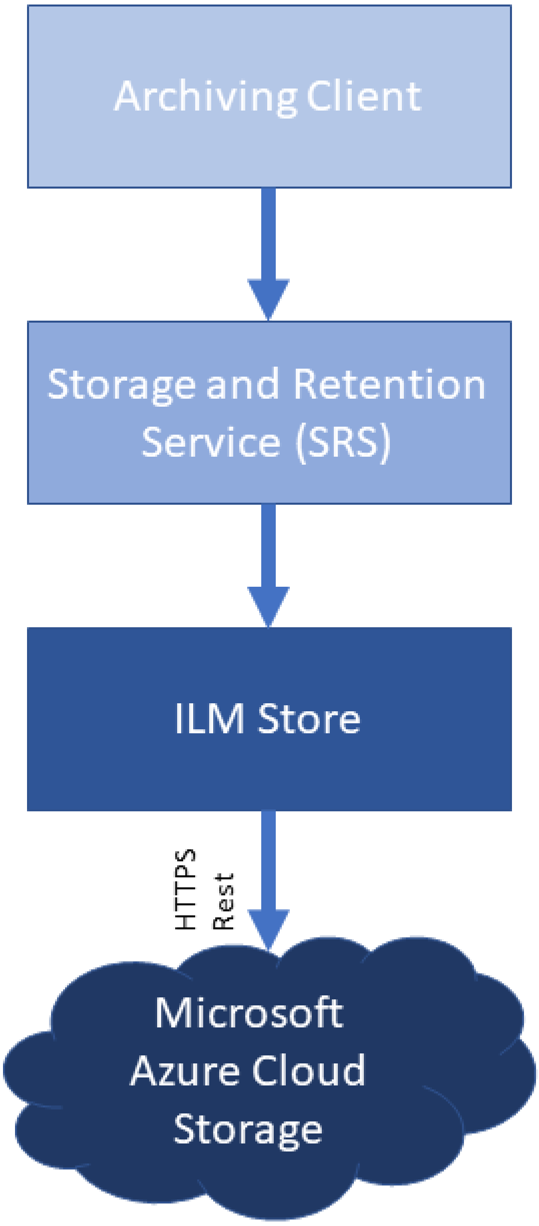

Archiving Client
Storage and Retention Service (SRS)
ILM Store
HTTPS
Rest
Microsoft Azure Cloud Storage

Figure 1: The SAP ILM Store with Microsoft Azure Storage

The SAP ILM Store with Microsoft Azure Storage

The system landscape can be configured in various ways, such as:

- The archiving client, the Storage and Retention Service (SRS), and the ILM Store reside on the same system.
- Using remote SRS to isolate the archiving client and the SRS.
- The archiving client and the SRS reside on the same system, while the ILM Store is on a separate system.

This guide explains how to configure the ILM Store with a Microsoft Azure storage account.

⚠ Caution

Once the ILM Store is set up and the operations have started, do not change the settings as it can lead to the loss of all stored information.

2 Prerequisites

Ensure that the following pre-requisites are met:

1. You use a SAP S/4HANA 2021 system or an ABAP PLATFORM 2021 system.
2. You have activated the business functions Information Lifecycle Management (`ILM`) and ILM Database Store (`ILM_STOR`).
3. You have a Microsoft Azure Blob Storage account set up.

> ⓘ Note
>
> When you create an application in the Microsoft Azure directory, note down the Client Secret, which is required for further configurations.

3 Authorizations

This section lists the authorizations required for configuring the ILM Store and storing files.

ILM Store Administration

Authorization Object	Field	Value
SILMSTOR	ACTVT	*02* (Change) *07* (Activate, Generate) *39* (Check)

Access to the ILM Store

You need a technical user with the necessary authorization to access the ILM Store and to upload files to the store. Assign a role to a user with the following authorizations:

Authorization Object	Field	Value
SILMSTOR	ACTVT	*16* (Execute)
S_DATASET	FILENAME	*
	PROGRAM	CL_ILM_STOR_DATASET===========CP, RILM_STOR_PUT_WORKER
	ACTVT	*6* (Delete), *33* (Read), *34* (Write)
S_DEVELOP	OBJTYP	*TABL*
	ACTVT	*07*, *40*
S_CTS_ADMI	CTS_ADMFCT	*TABL*
S_CTS_SADM	CTS_ADMFCT	*TABL*

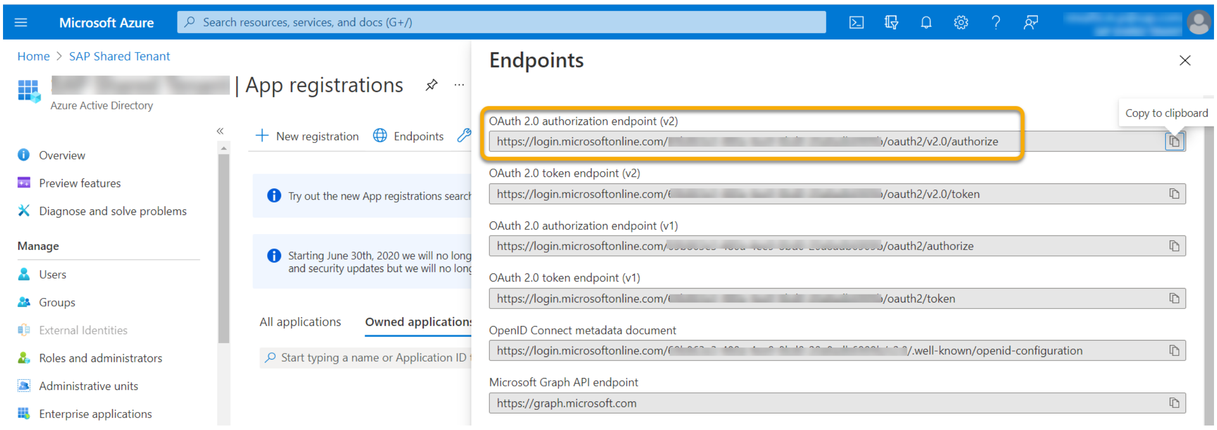
4 Storage Connection

Administrative data of the archive files is stored in the system database tables. The archive file data is stored as Blobs (Binary Large Object) in the configured Microsoft Azure Storage Account.

4.1 Exporting Certificates

The required certificates need to be exported to later import them into the SAP S/4HANA system. Access the Microsoft Azure Portal and log into your account. Note down the end points from the Microsoft Azure Portal as shown below.

Locate the OAuth 2.0 authorization endpoint (v2) as shown in fig. 2.



OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/[redacted]/oauth2/authorize

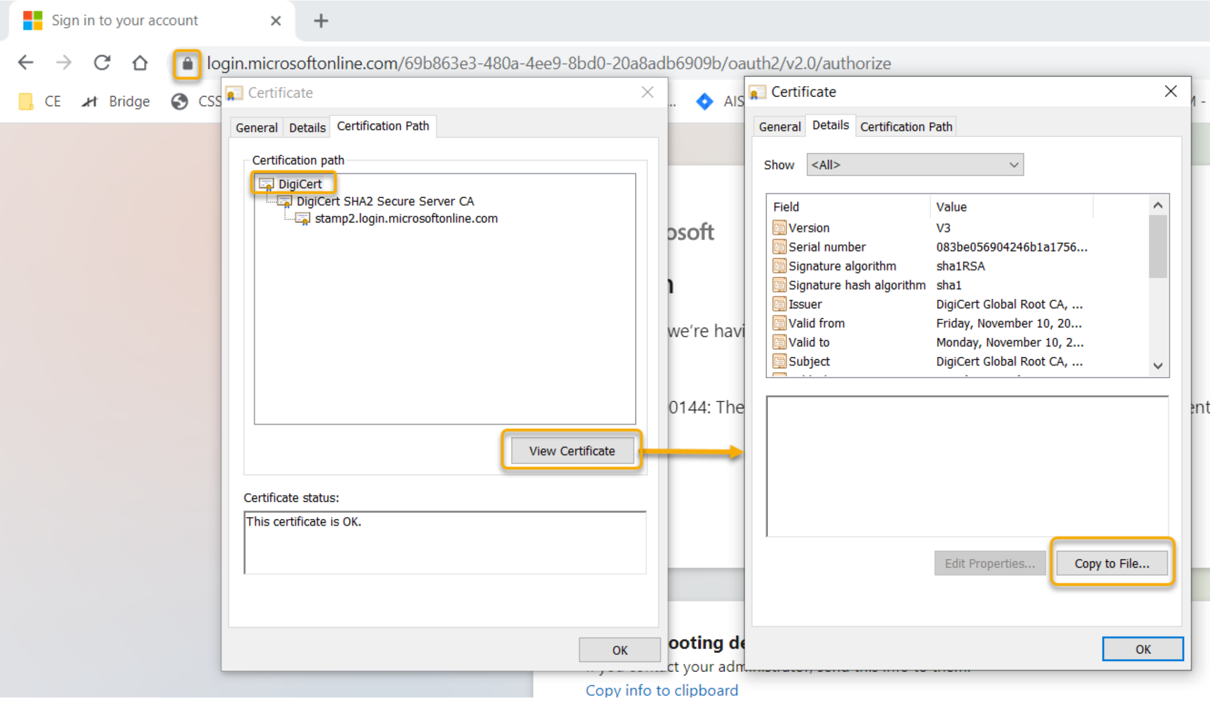
OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/[redacted]/oauth2/token

OpenID Connect metadata document
https://login.microsoftonline.com/[redacted]/.well-known/openid-configuration

Microsoft Graph API endpoint
https://graph.microsoft.com

Figure 2: Authorization Endpoint (V2)

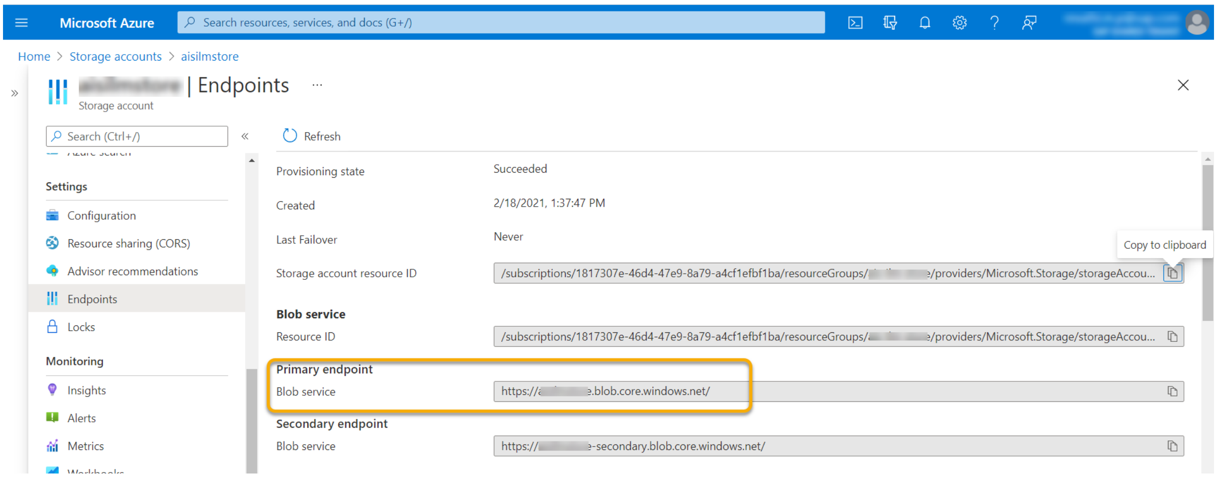
1. Copy the URL shown in fig. 2, paste it to your browser and press enter.
2. Click on the lock icon in the address bar.
3. Click on *Certificates* and a new window will open.
4. Go to the tab *Certification Path* (see fig. 3).
5. Select *Digi Cert*, click on *View Certificate* and a new window will open.
6. Go to *Details* and click on *Copy to File* (see fig. 3).
7. Save the certificate file (.CER) locally.



Field	Value
Version	V3
Serial number	083be056904246b1a1756...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	DigiCert Global Root CA, ...
Valid from	Friday, November 10, 20...
Valid to	Monday, November 10, 2...
Subject	DigiCert Global Root CA, ...

Figure 3: Download the Certificate with an Authorization Endpoint

Locate the Blob service of the primary endpoint as shown in fig. 4.



[redacted] | Endpoints

Provisioning state: Succeeded

Created: 2/18/2021, 1:37:47 PM

Last Failover: Never

Storage account resource ID: /subscriptions/1817307e-46d4-47e9-8a79-a4cf1efbf1ba/resourceGroups/[redacted]/providers/Microsoft.Storage/storageAccou...

Blob service

Resource ID: /subscriptions/1817307e-46d4-47e9-8a79-a4cf1efbf1ba/resourceGroups/[redacted]/providers/Microsoft.Storage/storageAccou...

Primary endpoint

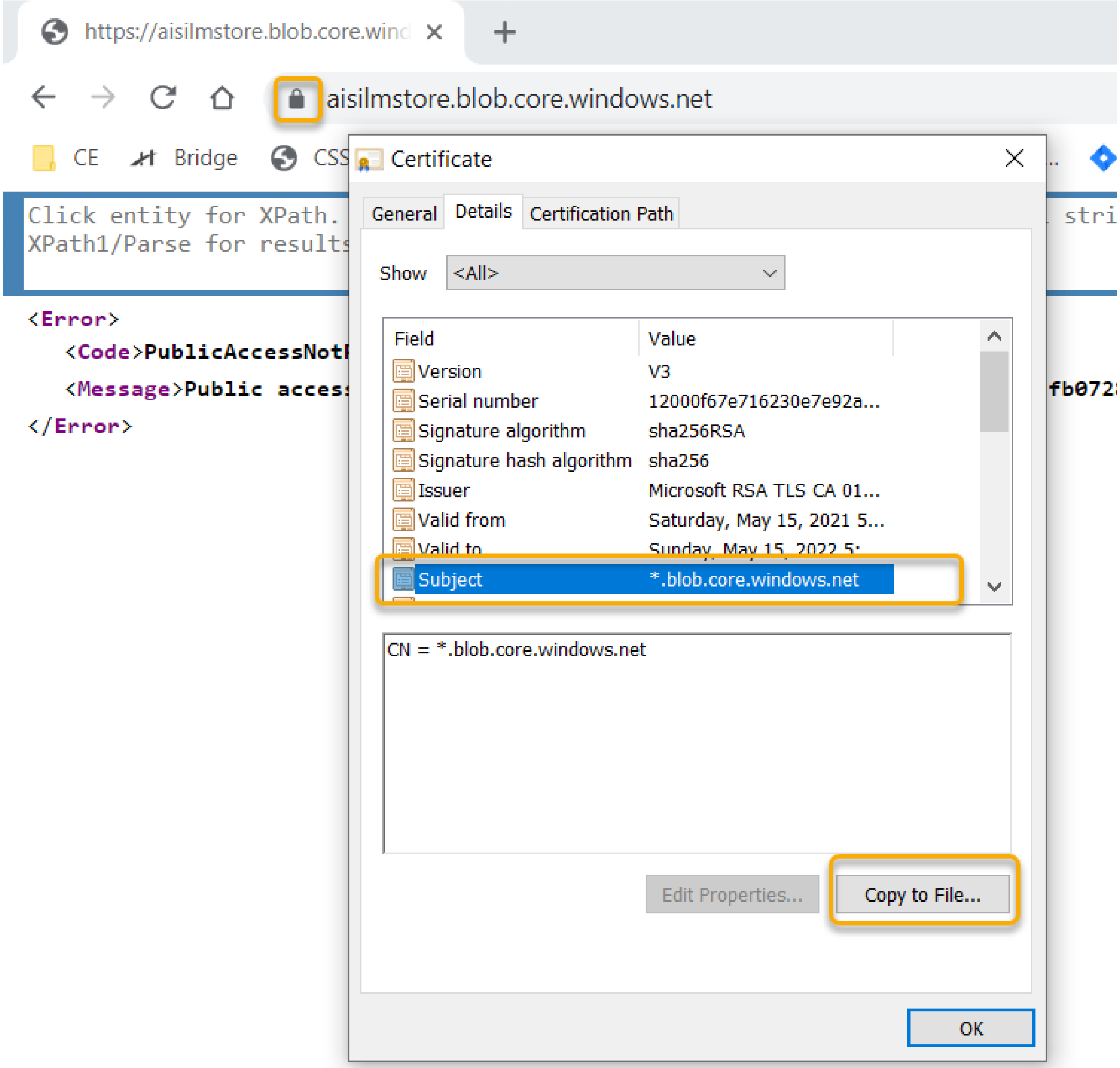
Blob service: https://[redacted].blob.core.windows.net/

Secondary endpoint

Blob service: https://[redacted]-secondary.blob.core.windows.net/

Figure 4: Primary Endpoint Blob Service

1. Copy the URL shown in fig. 3, paste it to your browser and press enter.
2. Click on the lock icon in the address bar.
3. Click on *Certificates* and a new window will open.
4. Go to the tab *Certification Path*.
5. Select *Digi Cert*, click on *View Certificate* and a new window will open.
6. Go to *Details* and click on *Copy to File* (see fig. 5).
7. Save the certificate file (.CER) locally.



```
Click entity for XPath.
XPath1/Parse for results
```

```
<Error>
    <Code>PublicAccessNot
    <Message>Public access
</Error>
```

Field	Value
Version	V3
Serial number	12000f67e716230e7e92a...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Microsoft RSA TLS CA 01...
Valid from	Saturday, May 15, 2021 5...
Valid to	Sunday, May 15, 2022 5:...
Subject	*.blob.core.windows.net

CN = *.blob.core.windows.net

Figure 5: Download the Certificate with the Primary Endpoint Blob Service

These two certificates will have to be uploaded to the ILM Store (see Importing Certificates [page 10]).

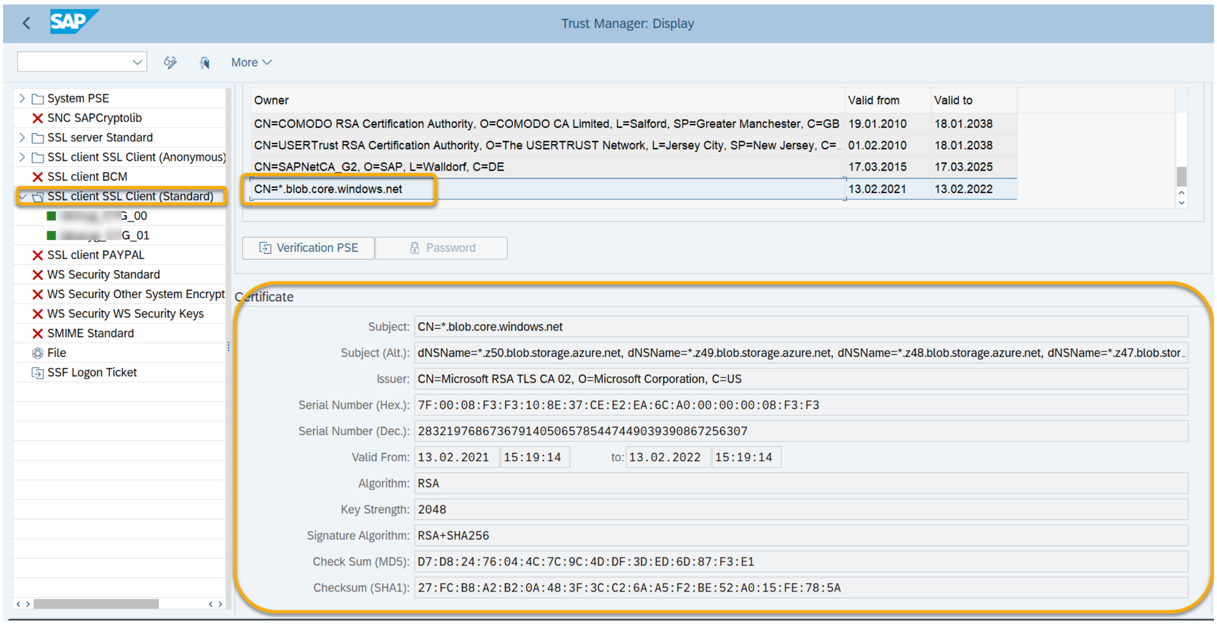
Next, log into the SAP S/4HANA system with a user with the necessary authorizations to configure the ILM Store.

4.2 Importing Certificates

In the SAP S/4HANA system, you need to import the previously exported certificates to establish a connection between the systems using HTTPS. To ensure a secure connection using the OAuth 2.0 client, you must use a SSL/TLS communication channel between your service provider (Microsoft Azure in this case) and the Application Server ABAP.

Follow the steps below to upload the certificates:

1. Start transaction `STRUST`.
2. Import the certificates downloaded in the previous step (see Exporting Certificates [page 8]).
3. Save the certificates under the node “SSL Client SSL Client (Standard)” (see fig. 6).



Owner	Valid from	Valid to
CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, SP=Greater Manchester, C=GB	19.01.2010	18.01.2038
CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, SP=New Jersey, C=…	01.02.2010	18.01.2038
CN=SAPNetCA_G2, O=SAP, L=Walldorf, C=DE	17.03.2015	17.03.2025
CN=*.blob.core.windows.net	13.02.2021	13.02.2022

Certificate

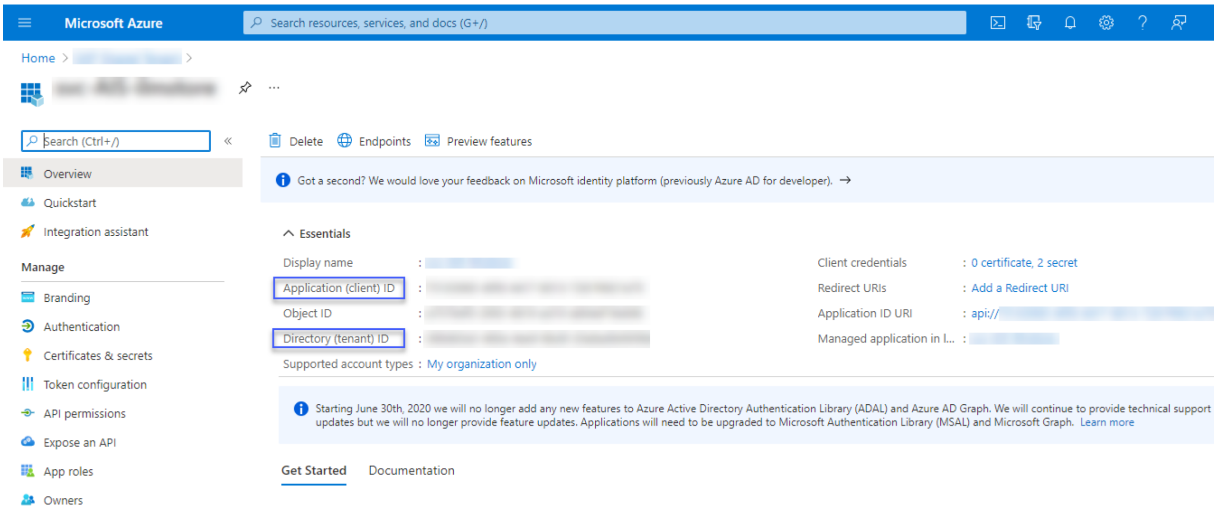
Subject: CN=*.blob.core.windows.net
Subject (Alt.): dNSName=*.z50.blob.storage.azure.net, dNSName=*.z49.blob.storage.azure.net, dNSName=*.z48.blob.storage.azure.net, dNSName=*.z47.blob.stor…
Issuer: CN=Microsoft RSA TLS CA 02, O=Microsoft Corporation, C=US
Serial Number (Hex.): 7F:00:08:F3:F3:10:8E:37:CE:E2:EA:6C:A0:00:00:00:08:F3:F3
Serial Number (Dec.): 2832197686736791405065785447449039390867256307
Valid From: 13.02.2021 15:19:14 to: 13.02.2022 15:19:14
Algorithm: RSA
Key Strength: 2048
Signature Algorithm: RSA+SHA256
Check Sum (MD5): D7:D8:24:76:04:4C:7C:9C:4D:DF:3D:ED:6D:87:F3:E1
Checksum (SHA1): 27:FC:B8:A2:B2:0A:48:3F:3C:C2:6A:A5:F2:BE:52:A0:15:FE:78:5A

Figure 6: Certificates Under the Standard Client Node

4.3 Configuring OAUTH for the ILM Store

Follow the steps below to configure OAUTH for the ILM Store:

1. Start transaction `OA2C_CONFIG` and create a new configuration.
2. Use the profile `ILMAZURE_STORAGE_OATUHPROF` and enter the values noted from the Microsoft Azure account (see fig. 9).
   Access the Microsoft Azure Portal and log into your account. Open the active directory application and note down the Client ID, Client Secret and Tenant ID as shown in fig. 7 and fig. 8. This is required to create an OAuth configuration in the SAP S/4HANA system.



Microsoft Azure | Search resources, services, and docs (G+/)

Home > [redacted] >

[redacted]

Delete | Endpoints | Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

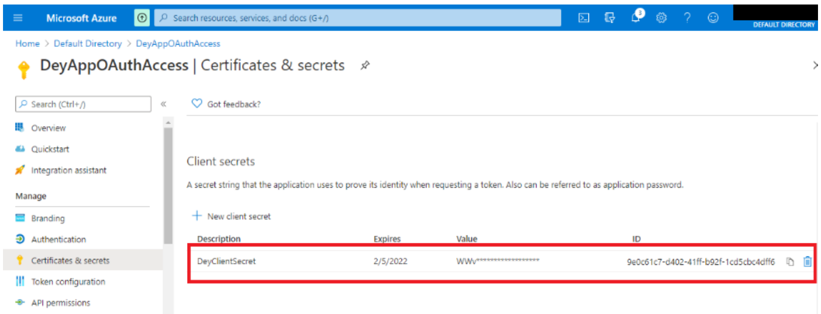
Essentials

Display name	: [redacted]	Client credentials	: 0 certificate, 2 secret
Application (client) ID	: [redacted]	Redirect URIs	: Add a Redirect URI
Object ID	: [redacted]	Application ID URI	: api://[redacted]
Directory (tenant) ID	: [redacted]	Managed application in l...	: [redacted]
Supported account types	: My organization only		

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Get Started | Documentation

Figure 7: Microsoft Azure Active Directory Parameter – Tenant ID



Microsoft Azure | Search resources, services, and docs (G+/) | [redacted] DEFAULT DIRECTORY

Home > Default Directory > DeyAppOAuthAccess

DeyAppOAuthAccess | Certificates & secrets

Got feedback?

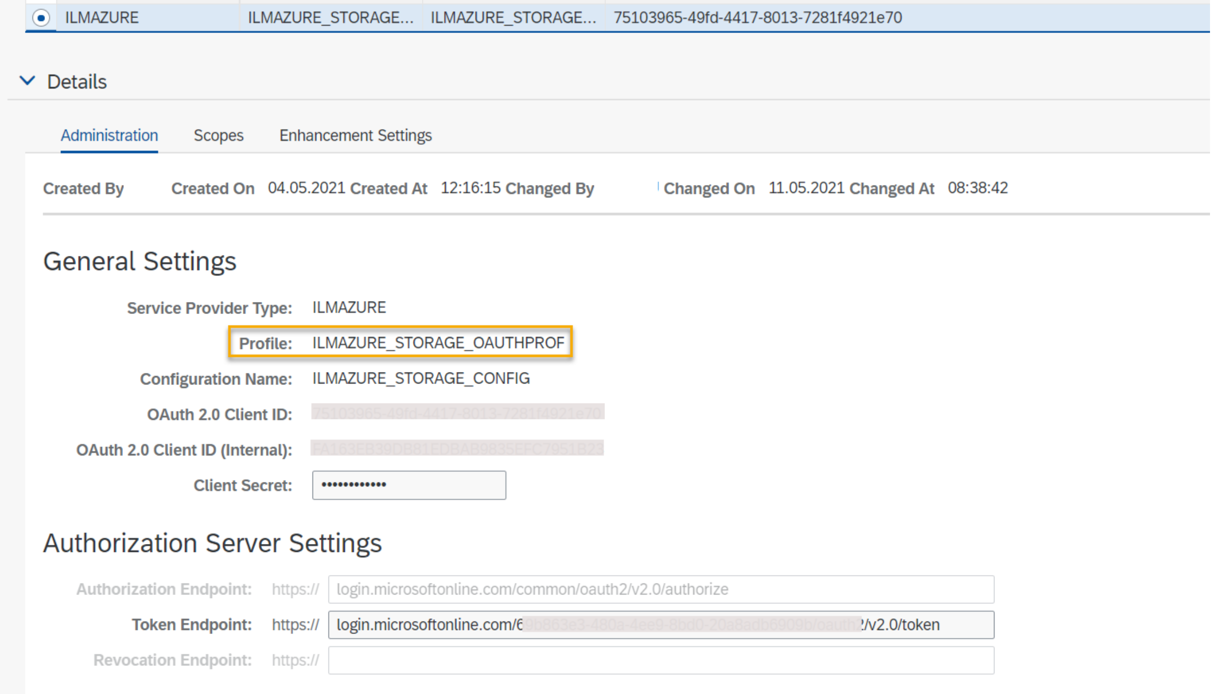
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
DeyClientSecret	2/5/2022	WWv******************	9e0c61c7-d402-41ff-b92f-1cd5cbc4dff6

Figure 8: Client ID and Client Secret of the Active Directory



● ILMAZURE | ILMAZURE_STORAGE... | ILMAZURE_STORAGE... | 75103965-49fd-4417-8013-7281f4921e70

Details

Administration | Scopes | Enhancement Settings

Created By | Created On 04.05.2021 | Created At 12:16:15 | Changed By | Changed On 11.05.2021 | Changed At 08:38:42

General Settings

Service Provider Type: ILMAZURE

Profile: ILMAZURE_STORAGE_OAUTHPROF

Configuration Name: ILMAZURE_STORAGE_CONFIG

OAuth 2.0 Client ID: [redacted]

OAuth 2.0 Client ID (Internal): [redacted]

Client Secret: ••••••••••••

Authorization Server Settings

Authorization Endpoint: https:// login.microsoftonline.com/common/oauth2/v2.0/authorize

Token Endpoint: https:// login.microsoftonline.com/6[redacted]/v2.0/token

Revocation Endpoint: https://

Figure 9: OAuth 2.0 Client Settings

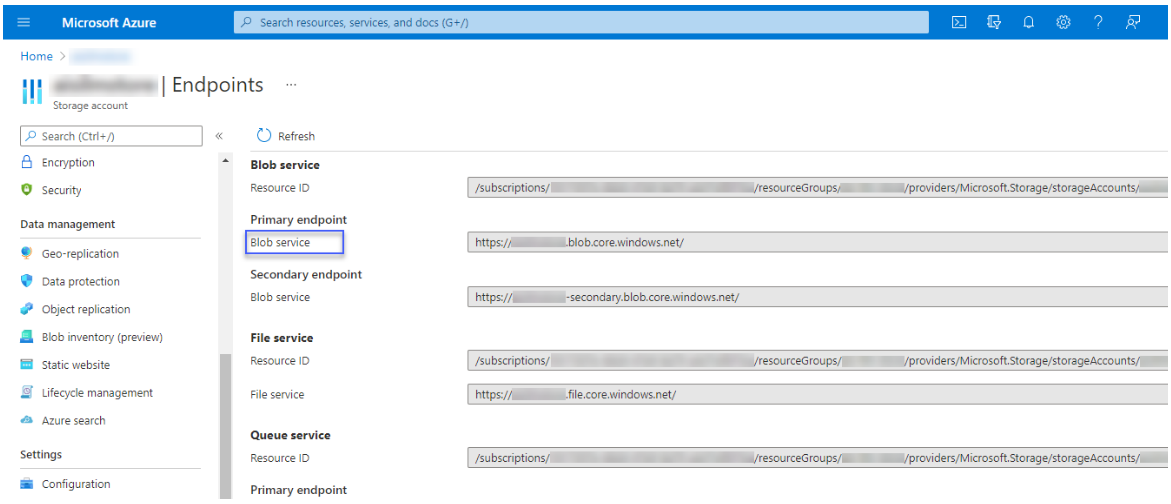
In the configurations, the Microsoft Azure Tenant ID is assigned to a Token endpoint, the Microsoft Azure application Client ID is assigned to an OAuth 2.0 Client ID and the Microsoft Azure application Client Secret is assigned to an OAuth 2.0 Client Secret (see fig. 9).

> ⓘ Note
>
> The Client Secret is renewed periodically at Microsoft Azure. When Microsoft Azure is updated, the Client Secret in `OA2C_CONFIG` is updated as well.

4.4 Creating the Remote Function Call (RFC)

1. Start transaction `SM59`.
2. Create a new RFC, choose a RFC destination and select connection type *G – HTTP Connections to External Server*.

   > ⓘ Note
   >
   > This RFC must be used to construct the primary endpoint as shown in fig. 10.



Home > [redacted]

[redacted] | Endpoints

Blob service

Resource ID: /subscriptions/[redacted]/resourceGroups/[redacted]/providers/Microsoft.Storage/storageAccounts/[redacted]

Primary endpoint

Blob service: https://[redacted].blob.core.windows.net/

Secondary endpoint

Blob service: https://[redacted]-secondary.blob.core.windows.net/

File service

Resource ID: /subscriptions/[redacted]/resourceGroups/[redacted]/providers/Microsoft.Storage/storageAccounts/[redacted]

File service: https://[redacted].file.core.windows.net/

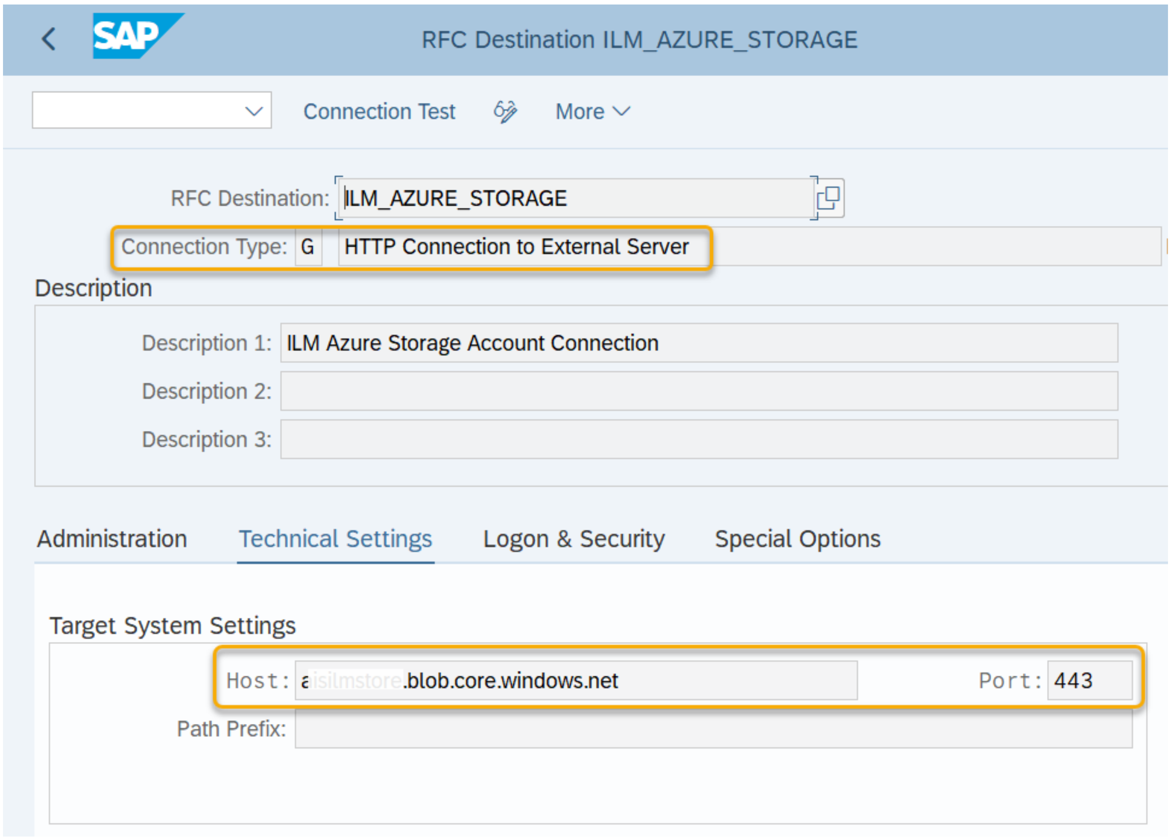
Queue service

Resource ID: /subscriptions/[redacted]/resourceGroups/[redacted]/providers/Microsoft.Storage/storageAccounts/[redacted]

Primary endpoint

Figure 10: Endpoint of the Storage Account in Microsoft Azure

3. In the tab *Logon and Security*, select *Active* for SSL.
4. Under *Special Options*, select *HTTP 1.1* as the HTTP version (see fig. 11 and fig. 12).



RFC Destination: ILM_AZURE_STORAGE

Connection Type: G HTTP Connection to External Server

Description

Description 1: ILM Azure Storage Account Connection

Description 2:

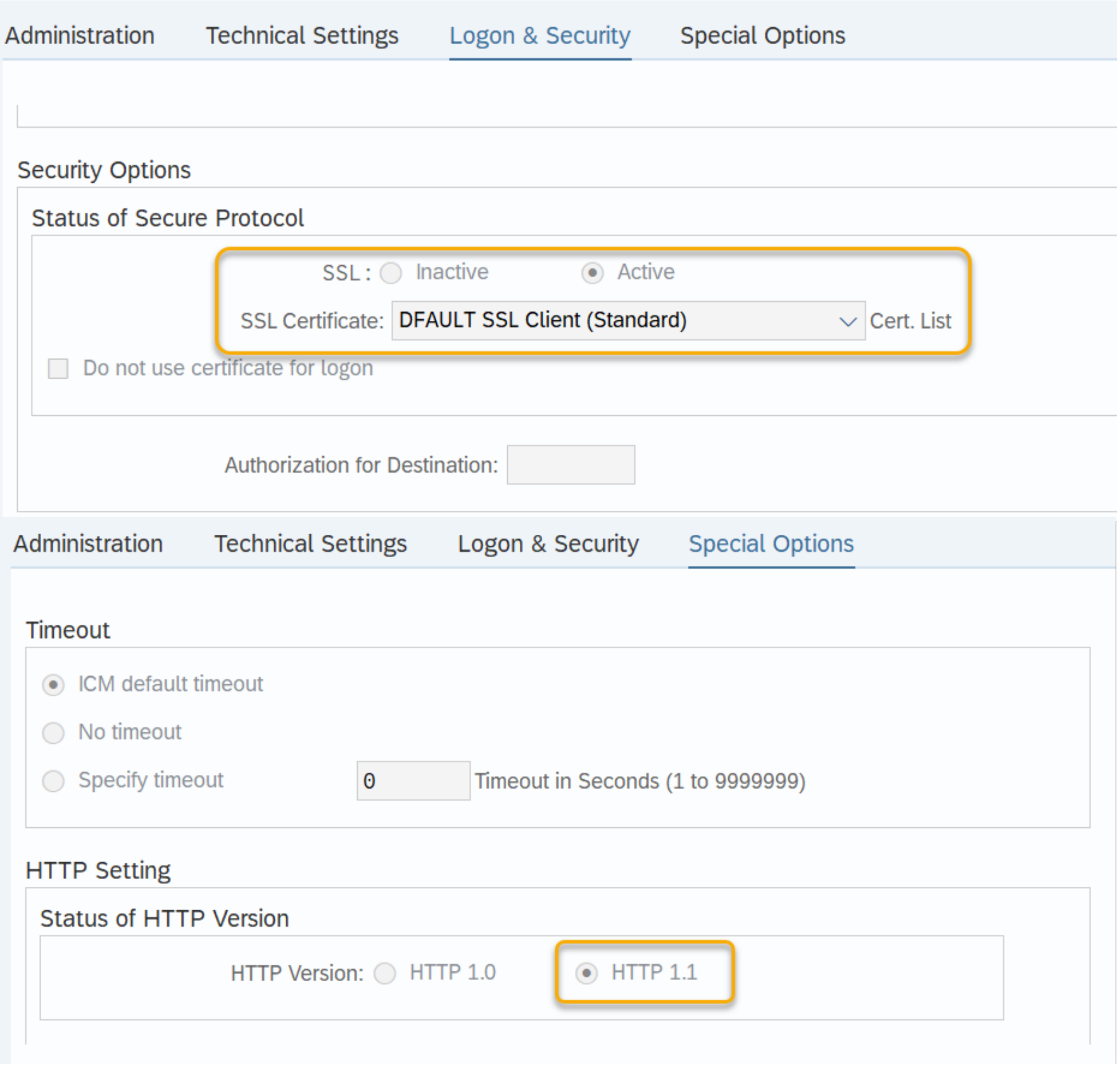
Description 3:

Target System Settings

Host: a[redacted].blob.core.windows.net Port: 443

Path Prefix:

Figure 11: RFC Destination



Security Options

Status of Secure Protocol

SSL : ○ Inactive ● Active

SSL Certificate: DFAULT SSL Client (Standard) Cert. List

□ Do not use certificate for logon

Authorization for Destination:

Timeout

● ICM default timeout

○ No timeout

○ Specify timeout 0 Timeout in Seconds (1 to 9999999)

HTTP Setting

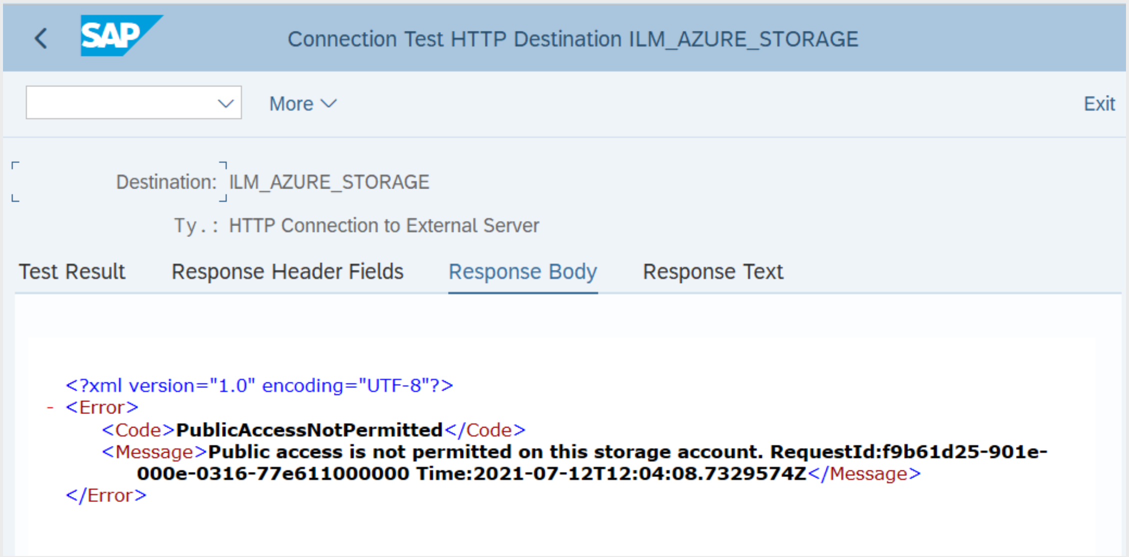
Status of HTTP Version

HTTP Version: ○ HTTP 1.0 ● HTTP 1.1

Figure 12: RFC Configurations

5. Save the changes.
6. Click on *Connection Test* and compare your test result to fig. 13.

> ⓘ Note
>
> Check if the connection is established. The connection test should return the message `Public Access not permitted`. This is the expected behavior based on the storage account setup with the value *Enable blob public access* set to false.



Destination: ILM_AZURE_STORAGE

Ty.: HTTP Connection to External Server

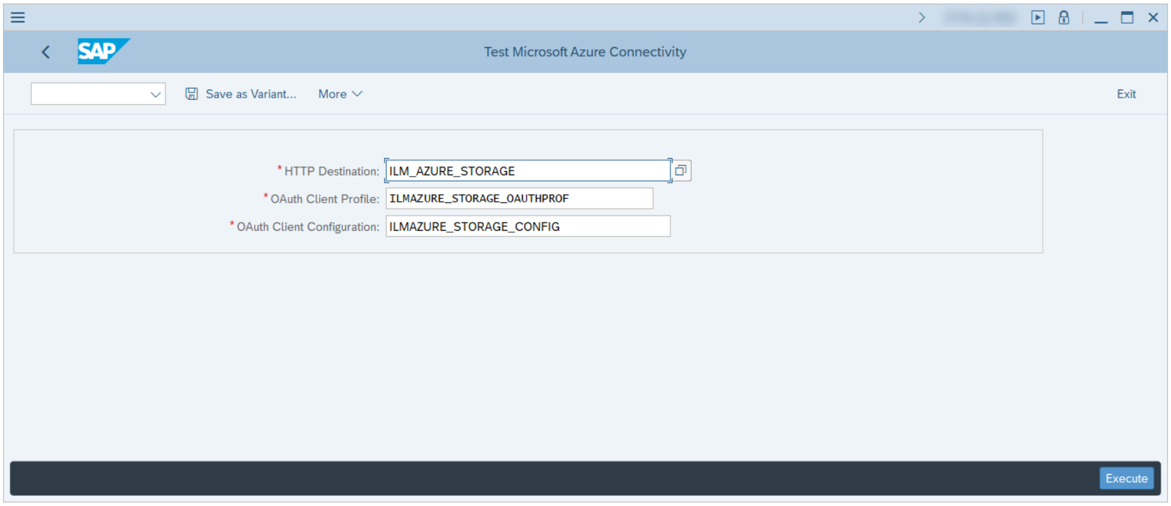
```
  <?xml version="1.0" encoding="UTF-8"?>
- <Error>
     <Code>PublicAccessNotPermitted</Code>
     <Message>Public access is not permitted on this storage account. RequestId:f9b61d25-901e-
        000e-0316-77e611000000 Time:2021-07-12T12:04:08.7329574Z</Message>
  </Error>
```

Figure 13: RFC Connection Test Result

4.5 Testing the Connection

Once the configurations in the system are completed, you can test the connection to the Microsoft Azure storage account. Follow the steps below:

1. In the store system, start transaction SE38.
2. Execute the report `RILM_STOR_TEST_AZURE` with the input parameters as shown in fig. 14.



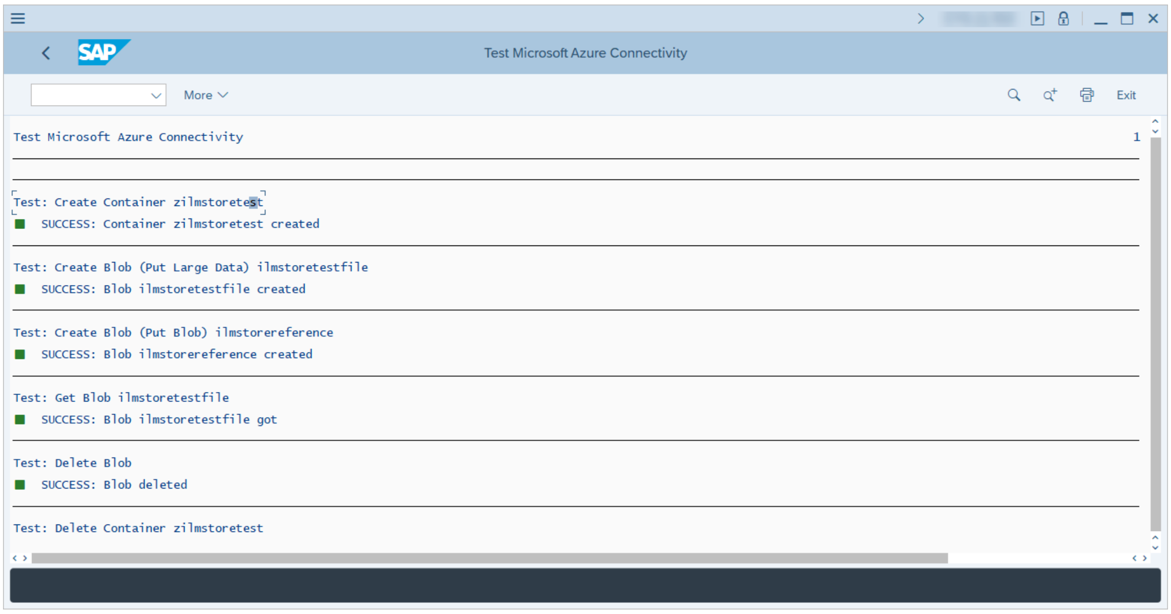
*HTTP Destination: ILM_AZURE_STORAGE

*OAuth Client Profile: ILMAZURE_STORAGE_OAUTHPROF

*OAuth Client Configuration: ILMAZURE_STORAGE_CONFIG

Figure 14: Test Report Input Parameters

3. Check if the test was successful and compare your result to fig. 14a.



```
Test Microsoft Azure Connectivity                                                    1

Test: Create Container zilmstoretest
🟩  SUCCESS: Container zilmstoretest created

Test: Create Blob (Put Large Data) ilmstoretestfile
🟩  SUCCESS: Blob ilmstoretestfile created

Test: Create Blob (Put Blob) ilmstorereference
🟩  SUCCESS: Blob ilmstorereference created

Test: Get Blob ilmstoretestfile
🟩  SUCCESS: Blob ilmstoretestfile got

Test: Delete Blob
🟩  SUCCESS: Blob deleted

Test: Delete Container zilmstoretest
```

Figure 15: Test Report Result

5 Customizing the Origin Settings

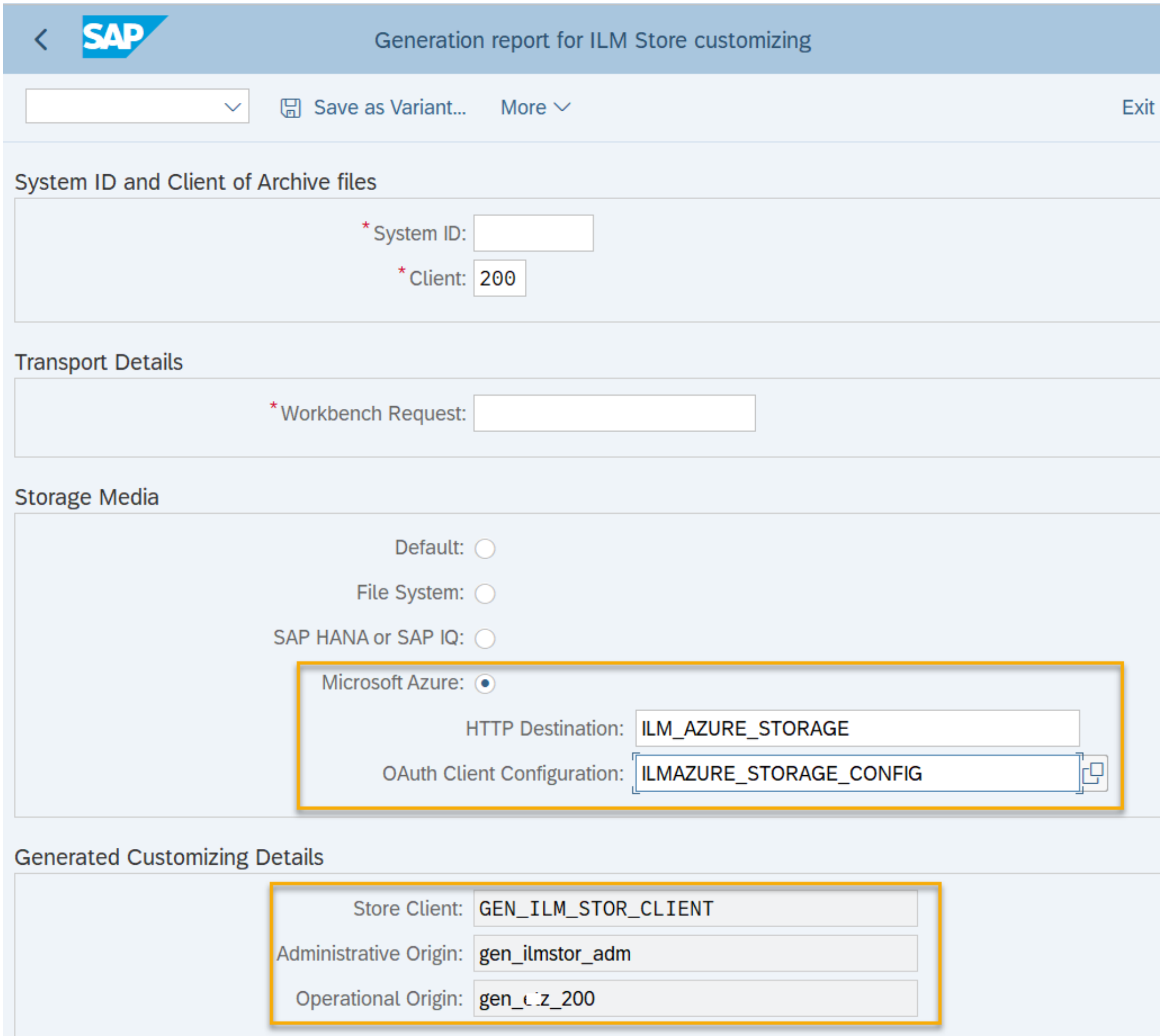
The origin is a central element in the configuration of the store. It serves as the identifier of the data source.

The customizing settings for the ILM Store can be generated using a report or they can be manually created.

5.1 Creating the Customizing Details Automatically

A simplified and automatic method to create the required settings for the ILM Store setup is enabled. Follow the steps below:

1. In the ILM Store system, start transaction `ILM_STOR_GEN_CUST`.
2. Enter the values for the input field (see fig. 15).
3. Select Microsoft Azure as the storage media.
4. Enter the details of the RFC destination and the OAuth configuration created earlier (see Creating the Remote Function Call (RFC) [page 13]) as shown in fig. 15.



Generation report for ILM Store customizing

System ID and Client of Archive files

*System ID:

*Client: 200

Transport Details

*Workbench Request:

Storage Media

Default: ○

File System: ○

SAP HANA or SAP IQ: ○

Microsoft Azure: ●

HTTP Destination: ILM_AZURE_STORAGE

OAuth Client Configuration: ILMAZURE_STORAGE_CONFIG

Generated Customizing Details

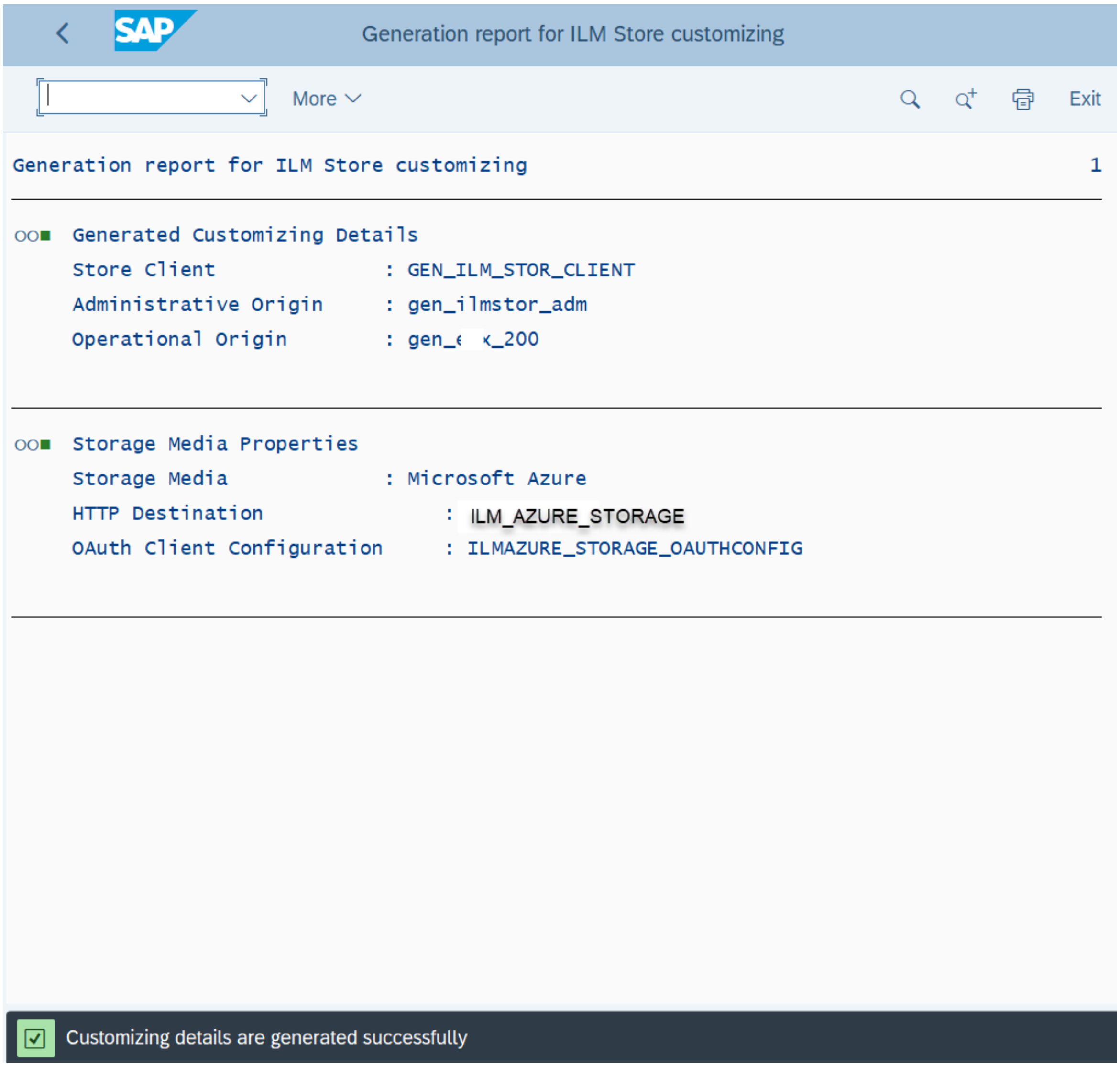
Store Client: GEN_ILM_STOR_CLIENT

Administrative Origin: gen_ilmstor_adm

Operational Origin: gen_[redacted]z_200

Figure 16: Generating the ILM Store Customizing

5. Click on *Execute*.
6. A result page with details of the created customizing values will be displayed as shown in fig. 16.



```
Generation report for ILM Store customizing                                  1

Generated Customizing Details
    Store Client               : GEN_ILM_STOR_CLIENT
    Administrative Origin      : gen_ilmstor_adm
    Operational Origin         : gen_[redacted]_200

Storage Media Properties
    Storage Media              : Microsoft Azure
    HTTP Destination              : ILM_AZURE_STORAGE
    OAuth Client Configuration    : ILMAZURE_STORAGE_OAUTHCONFIG
```

☑ Customizing details are generated successfully

Figure 17: Result of the Generation Report

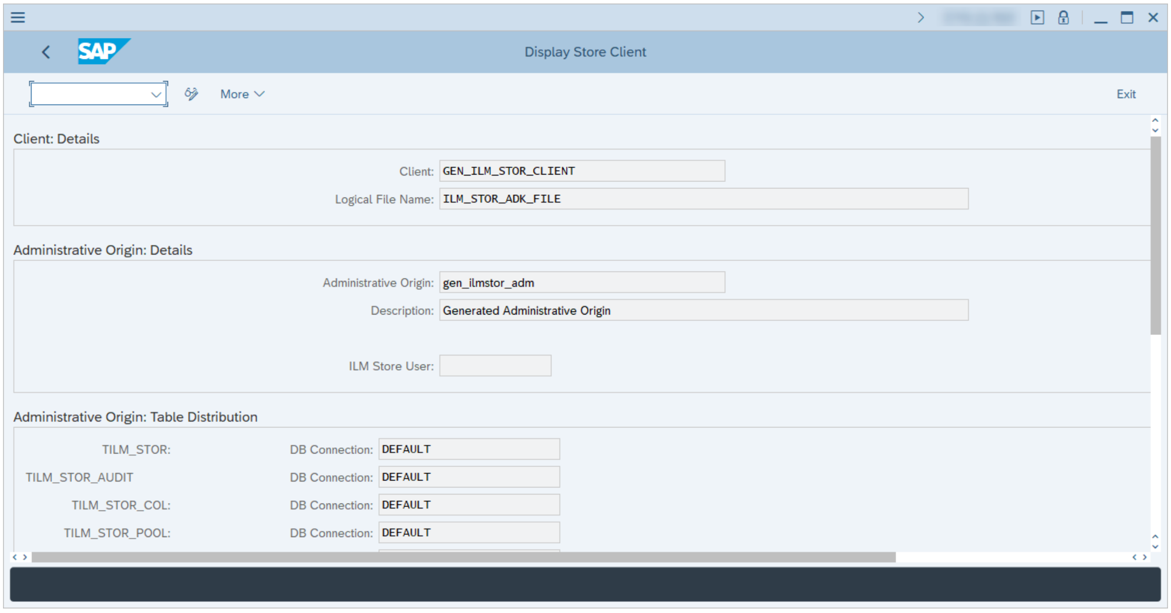
Once the configurations are generated in the system, perform a configuration test (see Testing the ILM Store Setup [page 25]).

5.2 Creating the Customizing Details Manually

If you have generated the customizing automatically (see Creating the Customizing Details Automatically [page 18]), this section is not required.

5.2.1 Administrative Customizing

1. In the ILM Store system, start transaction `ILM_STOR_ADM_CUST` or go to the *SAP NetWeaver Customizing Implementation Guide*, choose ❯ *ABAP Platform* ❯ *Application Server* ❯ *Basis Services* ❯ *Information Lifecycle Management* ❯ *ILM Store* ❯ *Define Settings for Administrative Customizing* ❯.
2. Click on *Create*.
3. Enter the name of the client and the *Logical File Name* (see fig. 17).
4. Specify a name and a description for the new *Administrative Origin* (see fig. 17).



Display Store Client

Client: Details

Client: GEN_ILM_STOR_CLIENT

Logical File Name: ILM_STOR_ADK_FILE

Administrative Origin: Details

Administrative Origin: gen_ilmstor_adm

Description: Generated Administrative Origin

ILM Store User:

Administrative Origin: Table Distribution

TILM_STOR:	DB Connection: DEFAULT
TILM_STOR_AUDIT	DB Connection: DEFAULT
TILM_STOR_COL:	DB Connection: DEFAULT
TILM_STOR_POOL:	DB Connection: DEFAULT

Figure 18: `ILM_STOR_ADM_CUST` Customizing

5. Click on *Add Operational Origin*.
6. In the new window, enter the name and description of the *Operational Origin*.
7. Chose *Microsoft Azure* as the Blob storage media.
8. Enter the HTTP Connection and the OAuth client configuration created in Exporting Certificates [page 8].

5.2.2 Operational Customizing

A set of properties can be defined at the operational origin level.

To maintain the properties for an operational origin, follow these steps:

1. Start transaction `ILM_STOR_OPR_CUST`.
2. Select the client you want to edit.
3. Click on *Execute*.
4. A set of properties are listed. You can maintain the required values for this list.

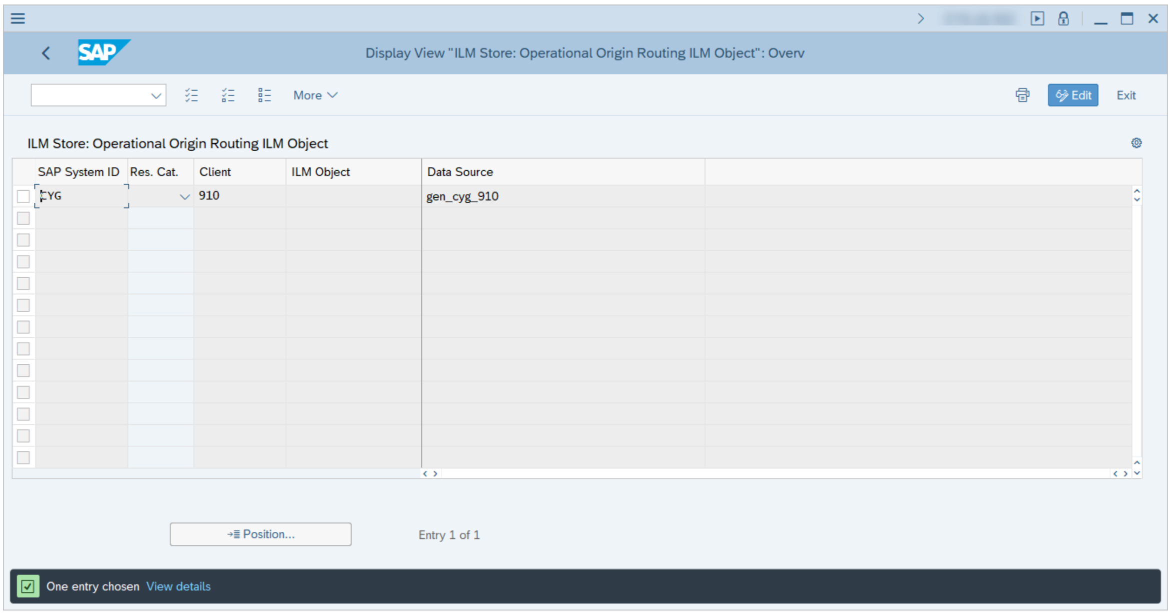
The other access path is via the *SAP NetWeaver Customizing Implementation Guide*, choose ❯ *ABAP Platform* ❯ *Application Server* ❯ *Basis Services* ❯ *Information Lifecycle Management* ❯ *ILM Store* ❯ *Define Settings for*

Operational Customizing ›. To do so, enter the value maintained in the Administrative Origin client and click on *Execute*.

5.2.3 Configuring the Routing Table

To configure the routing table, follow the steps below:

1. Start transaction `ILN_STOR_ADM_CUST` and click on *Configure Routing*.
2. Create an entry with the following details (see fig. 18):
   System ID: `<system_id>`
   Client: `<client>`
   Data Source: `<your operational origin>`



Display View "ILM Store: Operational Origin Routing ILM Object": Overv

ILM Store: Operational Origin Routing ILM Object

SAP System ID	Res. Cat.	Client	ILM Object	Data Source
CYG		910		gen_cyg_910

Entry 1 of 1

One entry chosen View details

Figure 19: Routing Table Parameters

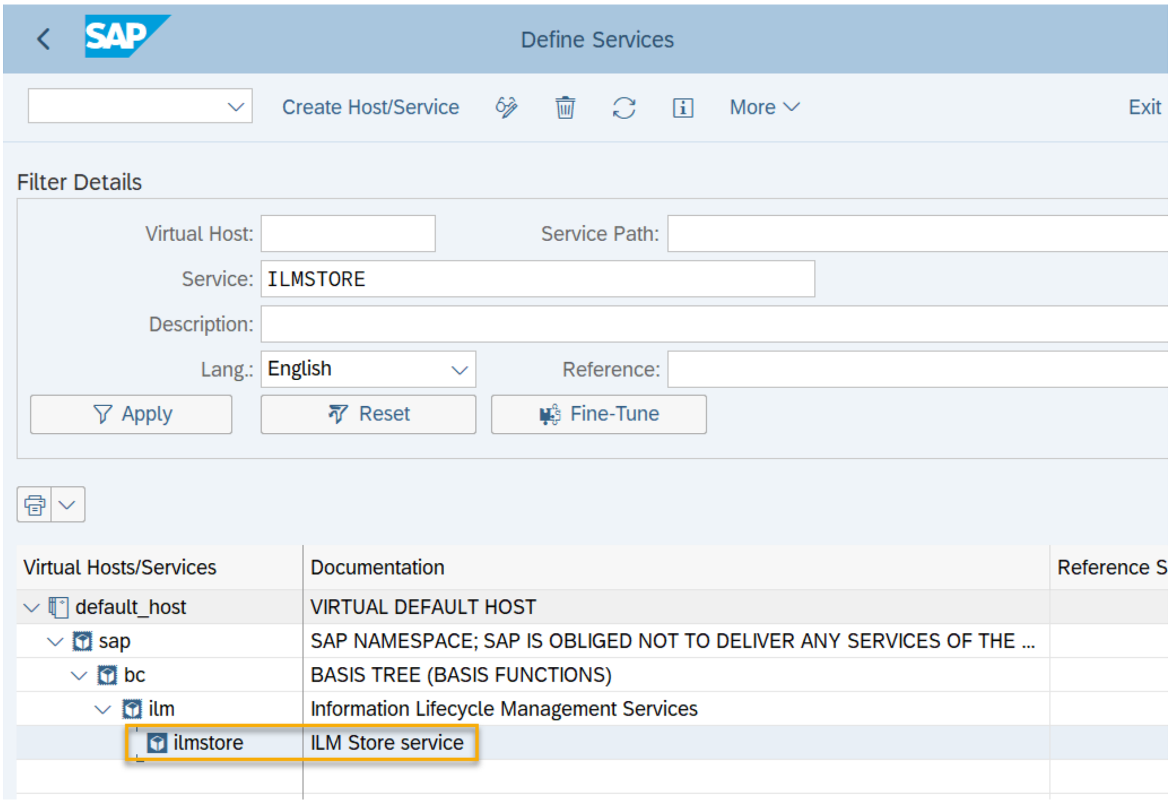
3. Save the changes.

6 Publishing the ILM Store

6.1 Activating the Internet Communication Framework (ICF) node for the ILM Store

Activate a service for the ILM Store.

1. Start transaction `SICF` and open the service `ILMSTORE` under node `ILM` as shown in fig. 19.



Virtual Host:

Service Path:

Service: ILMSTORE

Description:

Lang.: English

Reference:

Virtual Hosts/Services	Documentation	Reference S
default_host	VIRTUAL DEFAULT HOST	
sap	SAP NAMESPACE; SAP IS OBLIGED NOT TO DELIVER ANY SERVICES OF THE ...	
bc	BASIS TREE (BASIS FUNCTIONS)	
ilm	Information Lifecycle Management Services	
ilmstore	ILM Store service	

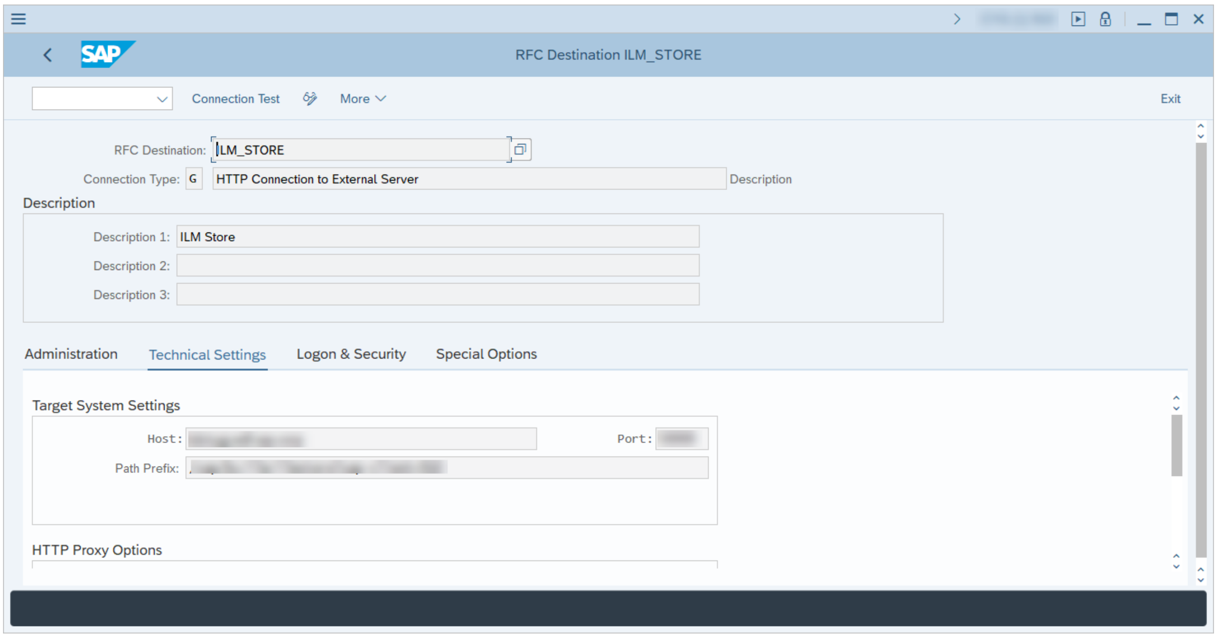
Figure 20: **`SICF`** Node for **`ILMSTORE`**

2. In the *Logon Data* tab, enter a user who has the authorization to access the ILM Store. For more information, refer to Authorizations [page 7].
3. Right click and activate the service.

6.2 Creating a RFC Destination

A communication channel is needed to establish a connection between the SAP system and the ILM Store.

1. Start transaction `SM59`.
2. Create a new HTTP connection to the external server (type G) (see fig. 20).
3. In the *Technical Settings* tab, enter the following values:
   - Target host
   - Service number (port) corresponding to your system.
   - Path prefix - This represents the connection between the destination and the ICF node.
     Enter the service path, which was defined in the `SICF` service `ILMSTORE` in the previous step (Test the service to obtain the path).
4. Save and perform a connection test.



RFC Destination ILM_STORE

RFC Destination: ILM_STORE

Connection Type: G HTTP Connection to External Server Description

Description

Description 1: ILM Store

Description 2:

Description 3:

Target System Settings

Host: [redacted] Port: [redacted]

Path Prefix: [redacted]

HTTP Proxy Options

Figure 21: RFC for the ILM Store

> ⓘ Note
>
> In case the SRS and the ILM Store are on two different systems, set up the RFC destination in the SRS system using the same procedure. The RFC destination in the ILM Store system is for testing purposes.

7 Testing the ILM Store Setup

After completing the setup, you must test the ILM Store.

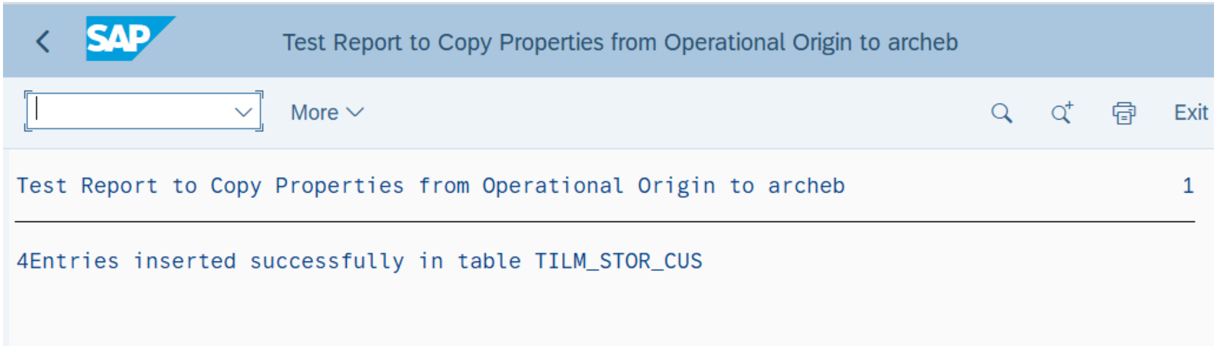
7.1 Origin Designed for Testing Purposes

SAP offers a test origin called ARCHEB, which you can use to test the ILM Store configurations.

It is mandatory to use test reports to check the functionality of the ILM Store.

Follow the steps below:

1. Start transaction SE38.
2. Execute the report RILM_STOR_TEST_COPY_ARCHEB.
3. Enter the operational origin created in Activating the Internet Communication Framework (ICF) node for the ILM Store [page 23] and click on *Execute*.
4. When successful, the results should match fig. 21.



SAP
Test Report to Copy Properties from Operational Origin to archeb
More
Exit

```
Test Report to Copy Properties from Operational Origin to archeb          1

4Entries inserted successfully in table TILM_STOR_CUS
```

Figure 22: Test Result for Operational Origin **ARCHEB**

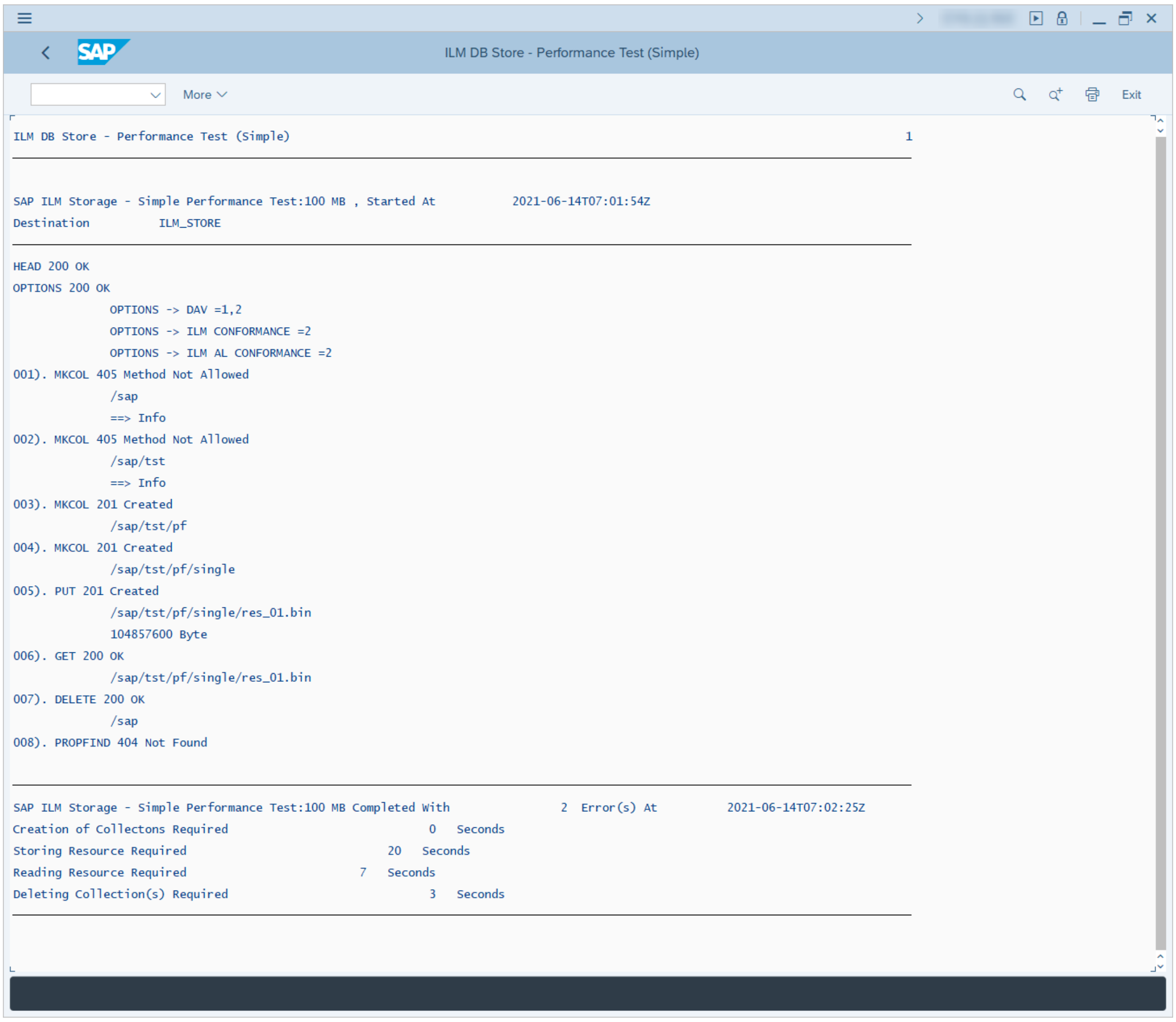
7.2 Test Reports

A set of reports are available to test the ILM Store setup and process.

7.2.1 Testing the Store Functionality

1. Start transaction SE38.
2. Execute report RILM_STOR_TEST_PF_SINGLE.

3. Enter the value of the RFC destination created earlier (see Creating a RFC Destination [page 24]) and click on *Execute*.
4. Compare the results to fig. 22.

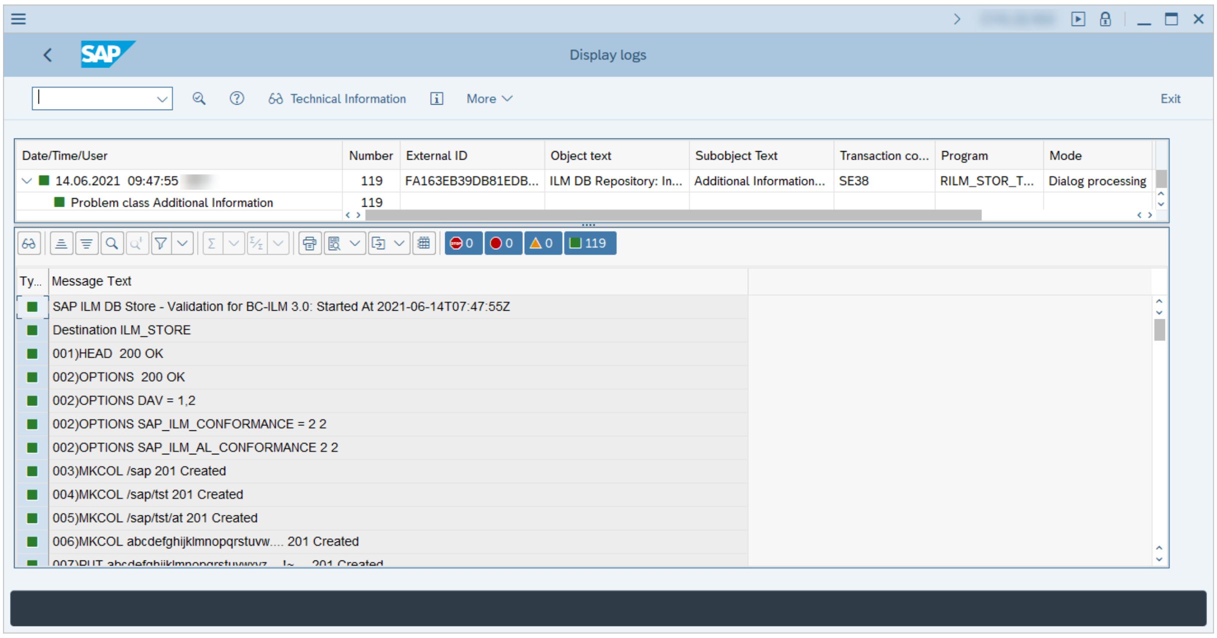


```
ILM DB Store - Performance Test (Simple)                                                                   1
_______________________________________________________________________________________________________________

SAP ILM Storage - Simple Performance Test:100 MB , Started At          2021-06-14T07:01:54Z
Destination         ILM_STORE
_______________________________________________________________________________________________________________
HEAD 200 OK
OPTIONS 200 OK
             OPTIONS -> DAV =1,2
             OPTIONS -> ILM CONFORMANCE =2
             OPTIONS -> ILM AL CONFORMANCE =2
001). MKCOL 405 Method Not Allowed
             /sap
             ==> Info
002). MKCOL 405 Method Not Allowed
             /sap/tst
             ==> Info
003). MKCOL 201 Created
             /sap/tst/pf
004). MKCOL 201 Created
             /sap/tst/pf/single
005). PUT 201 Created
             /sap/tst/pf/single/res_01.bin
             104857600 Byte
006). GET 200 OK
             /sap/tst/pf/single/res_01.bin
007). DELETE 200 OK
             /sap
008). PROPFIND 404 Not Found

_______________________________________________________________________________________________________________
SAP ILM Storage - Simple Performance Test:100 MB Completed With            2  Error(s) At         2021-06-14T07:02:25Z
Creation of Collectons Required                          0    Seconds
Storing Resource Required                           20    Seconds
Reading Resource Required                       7    Seconds
Deleting Collection(s) Required                          3    Seconds
_______________________________________________________________________________________________________________
```

Figure 23: Expected Output for Report **`RILM_STOR_TEST_PF_SINGLE`**

7.2.2 Testing the ILM Store Customizing

1. Start transaction `SE38`.
2. Execute report `RILM_STOR_TEST_AT`.
3. Enter the RFC destination created earlier (see Creating a RFC Destination [page 24]) and click on *Execute*.
4. Compare the results to fig. 23.



Date/Time/User	Number	External ID	Object text	Subobject Text	Transaction co...	Program	Mode
🟩 14.06.2021 09:47:55 [redacted]	119	FA163EB39DB81EDB...	ILM DB Repository: In...	Additional Information...	SE38	RILM_STOR_T...	Dialog processing
🟩 Problem class Additional Information	119						

Ty...	Message Text
🟩	SAP ILM DB Store - Validation for BC-ILM 3.0: Started At 2021-06-14T07:47:55Z
🟩	Destination ILM_STORE
🟩	001)HEAD 200 OK
🟩	002)OPTIONS 200 OK
🟩	002)OPTIONS DAV = 1,2
🟩	002)OPTIONS SAP_ILM_CONFORMANCE = 2 2
🟩	002)OPTIONS SAP_ILM_AL_CONFORMANCE 2 2
🟩	003)MKCOL /sap 201 Created
🟩	004)MKCOL /sap/tst 201 Created
🟩	005)MKCOL /sap/tst/at 201 Created
🟩	006)MKCOL abcdefghijklmnopqrstuvw.... 201 Created
🟩	007)PUT abcdefghijklmnopqrstuvwxyz ... l~ 201 Created

Figure 24: Expected Output for Report **`RILM_STOR_TEST_AT`**

7.3 Application Logs

The application log object for the ILM Store is `ILM_STOR`. Start transaction `SLG1` and enter the object `ILM_STOR` to see the logs of all operations performed in the store.

8 Storage and Retention Service (SRS)

The Storage and Retention Service (SRS) is needed to store ILM enabled archive files in the ILM Store.

To use the SRS for managing ILM Stores, you need to activate it in the application system.

8.1 Activating the SRS

To activate the SRS, the following options are available:

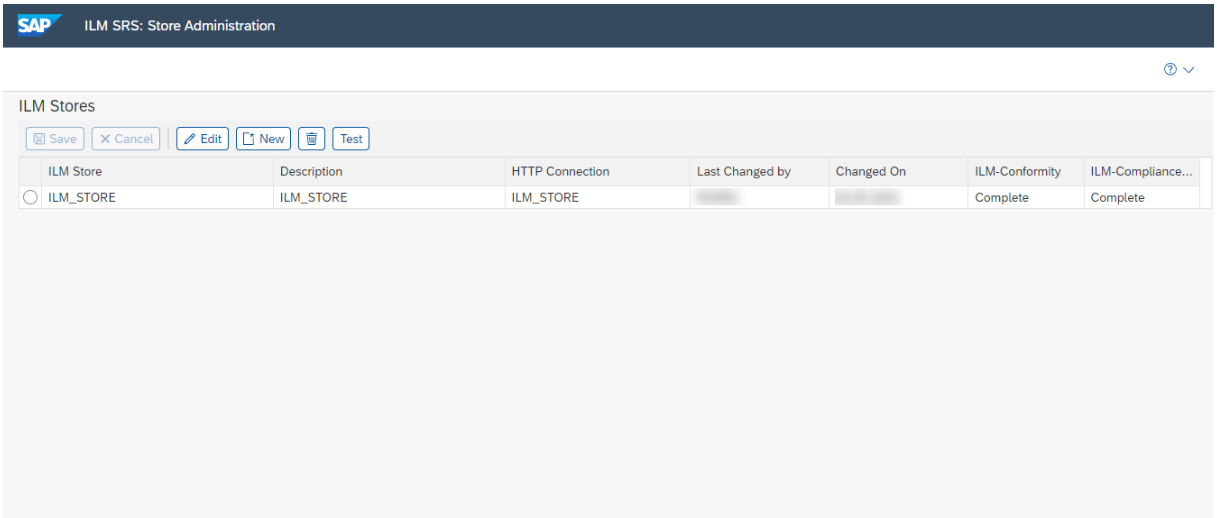
- Activate the SRS that runs locally in the application system.
- Activate the SRS that runs on a separate (remote) system. For this option, you need a HTTP connection between the relevant systems.

For more information, refer to the Installation and Configuration Guide for the ILM Store.

8.2 Creating an ILM Store with the SRS Administration

You can create ILM Stores which are further configured to connect to storage media linked via RFC connections. Follow the steps below:

1. Start transaction `ILMSTOREADM`.
2. Create a new entry.
3. Enter the values for the ILM Store:
   Name: an identifying name for the store
   Description: descriptive text
   HTTP Connection: the previously created RFC destination (see Creating a RFC Destination [page 24])
4. Save the changes (see fig. 24).



	ILM Store	Description	HTTP Connection	Last Changed by	Changed On	ILM-Conformity	ILM-Compliance...
○	ILM_STORE	ILM_STORE	ILM_STORE	[redacted]	[redacted]	Complete	Complete

Figure 25: ILM Store Creation

This store can further be used for ILM rule maintenance in transaction `IRMPOL`. For more information, refer to Editing Retention Rules.

8.3 Troubleshooting

If you run into issues, access the troubleshooting blog to find a list of common issues.

For further support, report an incident in the application component `BC-ILM-STO`.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon ➦ : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon ➦: You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP